

1

**ABSTRACT.**

2

3

4 A key establishment protocol includes the generation of a value of  
5 cryptographic function, typically a hash, of a session key and public information. This  
6 value is transferred between correspondents together with the information necessary to  
7 generate the session key. Provided the session key has not been compromised, the  
8 value of the cryptographic function will be the same at each of the correspondents.  
9 The value of the cryptographic function cannot be compromised or modified without  
10 access to the session key.

11

12